

The Interagency Advisory Board (IAB) meeting convened on Tuesday, April 17, 2006 at 9:15 AM at the Sheraton National Hotel in Arlington. After opening remarks by Randy Vanderhoof of the Smart Card Alliance (SCA) and Neville Pattinson of Axalto, the meeting was opened by Mike Butler, the IAB Chair, and followed by presentations:

A. Review of FIPS-201 Implementation Challenges - Mike Butler (IAB). Key Points:

- Since last IAB meeting, progress has been made addressing the identified technical issues/challenges.
- 4 issues have been resolved:
 - #1: Same OID for PIV Auth Key and CAC Signature Key
 - #3: Read Binary vs. Get Data
 - #5: Expiration Date Consistency
 - #10: Required use of PIN to access public key
- 5 issues have resolutions in progress
 - #2: Lack of guidance regarding security object
 - #4: CHUID buffer length
 - #7: Guidance for digital camera interface used at enrollment
 - #8: Transitional vs. End State – 2 byte vs. 3 byte tags in data model
 - #9: Required location for serial code on card (top vs. bottom)
- 1 issue has yet to receive action
 - #6: PIV Auth Key certificate & NACI Indicator
- The National Institute of Standards and Technology (NIST) is seeking agency input regarding whether full review of FIPS-201 is needed.
 - Agencies should identify specific provisions that require review and state reasoning for recommendation.
 - Deadline for responding to this request is June 16, 2006. Please send responses to wbarker@nist.gov and copy hildegard.ferraiolo@nist.gov

B. DoD Pre-Issuance Specification – Toni Cieri (IAB). Key Points:

- In this short educational brief, Mr. Cieri elaborated on the imperative for a pre-issuance specification. He highlighted the DoD's work in drafting a pre-issuance specification, and the business drivers for why it is important to have one.
- It is the building block for both key and cardstock management
- It documents Card Issuer's requirements and expectations for Card Manufacturer
- It outlines process for automated data transfer between the two
- It identifies key management requirements for transmitting non-PKI keys

C. Product Submissions to FIPS 201 Compliance Lab - Ramaswamy Chandramouli (Mouli) - (NIST). Key Points:

- Mouli provided an update of recent efforts in support of the NIST PIV Program (NPIVP):
 - To date, 11 interim designated test facilities have been stood up that are all Cryptographic Module Validation Program (CMVP) certified labs

- Converted labs from interim designation to formal accreditation
- 2 labs are actively testing PIV products, and another may join soon
- Mouli also touched on the products that are under the NPIVP Validation Scope:
 - PIV Card Applications – end-point command interfaces as defined in SP 800-73, Ch. 7
 1. Must pass SP 800-73-1 interface tests and FIPS 140-2 crypto module tests
 - PIV Middleware – end-point client application programming interfaces (API) as defined in SP 800-73, Ch. 6
 1. Must pass SP 800-73-1 interface tests
- NPIVP – Key Events & Artifacts
 - SP 800-85A documents derived test requirements and test assertions
 - NIST provides testing toolkit to NPIVP labs
 - Labs submit test reports to NIST/NPIVP
 - NPIVP validates test results, issues certificates, maintains validation lists
- Current Validation Status
 - PIV Card Application – 3 under test at labs, 1 issued cert, 1 under review
 - PIV Middleware – 5 under test at labs
- More information (such as Validation & Pre-Validation Lists) can be found at the NIST PIVP website: www.nist.gov/npivp

D. Status Update: ISO/IEC 24727, *Identification cards - Integrated circuit cards programming interfaces* - Bill MacGregor (NIST). Key Points:

- Mr. MacGregor started by assuaging people's fears by explaining that this initiative will not change rules on PIV, and that the earliest it will come into the marketplace is 2008.
- However, this initiative does add innovations for discovery & access control. Working with the overall philosophy that access control trumps discovery.
- The goal is to allow independent, interchangeable implementations.
- ISO/IEC 24727 work assigned to SC 17, Workgroup 4, Task Force 9 with active participation by Australia, Finland, France, Germany, Japan, Netherlands, UK, and US (chair)
- More at www.sc17.com & comelec.afnor.fr/iso/iec/jtc1/sc17/wg4

E. Alternative Biometric Modalities for PIV – Walter Hamilton (IBIA). Key Points:

- SP 800-76 neither requires nor precludes the use of:
 - The PIV Card fingerprint templates;
 - Specific authentication paradigms such as match-on-card;
 - Data from other biometric modalities (e.g., hand geometry, iris, etc.);
 - Data formatted according to other standards;
 - Data whose format is proprietary or otherwise undisclosed.
- Mr. Hamilton elaborated on the pros and cons of alternative biometric configurations for physical access. In particular, he spoke about the following paradigms:

- Match Off Card to Standard Fingerprint Template Stored On Card
- Match Off Card to Alternative Biometric Template Stored Off Card
- Match Off Card to Alternative Biometric Template Stored On Card
- Match On Card to Alternative Biometric Template Stored On Card
- IBIA recommendations to NIST for Physical Access Control Applications:
 - Remove PIN requirement for reading interoperable fingerprint templates on PIV card
 - Allow access to fingerprint templates through the contactless interface
- Conclusions
 - FIPS 201 allows a lot of flexibility in implementing biometric authentication for intra-agency access control
 - Operational use of alternative biometrics for physical and logical access control is allowed in FIPS 201
 - Given restrictions on use, interoperable templates will likely only be used at visitor control centers to verify that a visiting agency employee is the rightful owner of the PIV card
 - Consider the use of alternative biometrics – particularly for physical access control systems

F. HSPD-12 Document Revision Progress - Ramaswamy Chandramouli (Mouli) - (NIST). Key Points:

- NIST has issued a request for comments to HSPD-12 Leads seeking agency input regarding whether full review of FIPS-201 is needed.
- Recommendations will be evaluated in context of improving security, privacy, interoperability, operational effectiveness, cost efficiency, and standards stability.
- Deadline for responding to this request is June 16, 2006.
- Responses sent to wbarker@nist.gov with copy to hildegard.ferraiolo@nist.gov

G. FIPS 201 Evaluation Program - April Giles (GSA). Key Points:

- Ms. April Giles provided an update on the various initiatives associated with the FIPS 201 Evaluation Program:
- Card/Reader Interoperability Task - 99% complete
 - Test fixture prototype delivered
 - Card/reader requirements done (on 7th draft)
- Lab Development Task - 60% complete
 - Lab Specification Draft completed
 - Supplier Login applications accepted
 - 6 of 20 Categories ready for applications
 - Test Fixture software revised
 - Next major milestone
 - Website tool update
 - Evaluation Program Technical Working Group (EPTWG) review/comment on card & reader approval procedures

- Ms. Giles also informed the group that they are accepting Approved Products List (APL) early applications:
 - There is no fee, and it will be first-in and first-out with a cap per category.
 - However, since this will be used to validate the approval process suppliers must be flexible
- Ms. Giles concluded by making a call for industry support in a new working group.
 - Looking for IDMS/CMS suppliers to help outline CMS/IDMS requirements
 - Virtual meetings (1hour) weekly
 - To participate, contact april.giles@gsa.gov or 202.501.1123.
- More at www.smart.gov/fips201apl

H. Physical Access Synergy Of PAIIWG/SCA/SIA - Dwayne Pfeiffer (SCA) & Rob Zivney (SIA). Key Points:

- FIPS 201 and special publication are *normative* documents; meanwhile, documents like the PACS 2.2 are *informative*, except where specifically referenced (e.g., CHUID). Thus, the first focus should be on the normative documents, and in particular, SP800-73-1 Draft.
- Issues still exist with SP 800-73-1. The group reviewed the document during comment period, submitted comments, but they were probably too late for NIST to incorporate their changes. Remaining conflicts:
 - Read Binary vs. Get Data
 - 2 Byte vs. 3 Byte Addressing
 - Transitional vs. End Point
 1. Only End Point is Interoperable
 2. Transitional is NOT “Part Way to End Point”:
 3. Industry to “Focus” on End Point, though some readers can “Read All”
 - TIG SCEPACS
 1. v2.2 is normative, but only with regard to the CHUID
 2. v2.3 is informative
 - PACS Installed Base
 1. No reader-to-PACS protocol is specified
 2. 26 bit Wiegand is the most common protocol
 3. FASC-N is too large for most PACS, other compatibility issues exist
 4. PIV implementation may require replacement of PACS installed base
- Securities Industry Association (SIA) is publishing new PACS Standards
 - Data Model Focused on Interoperability
 - Incorporating FIPS 201 PIV Constructs: card, reader, PACS, IDMS, CMS
 - Process is open, and all can participate.
- The panel concluded by providing the PACS Synergy accomplishments:

- Made decision to keep GUID all zeros for now, use IPv6 or other number later
- Updated PACS v2.2 to v2.3
- Continued support to GSA's EPTWG
- Submitted comments on SP 800-73-1
- Working with GSA on PIV test Card solution, but there is a need for PIV Test Cards to continue to make progress.

I. Backend Authentication Scheme Working Group Final Report - Tim Baldrige (NASA). Key Points:

- Mr. Baldrige announced that there would be a government-only session of the Backend Authentication Scheme Work Group (BASWG) following the conclusion of the IAB meeting from 12:00 PM to 1:30 PM in a Smart Card Alliance reserved conference room.

J. Lessons Learned – Army Enterprise Rollout of Readers and Middleware - Greta Lehman (DMDC). Key Points:

- Ms. Lehman provided insights and lessons learned from her previous experience leading the Army rollout of readers and middleware from 2001 through 2005.
- Common Access Card/Public Key Infrastructure 2001-2004
 - Fielded 818,584 card readers
 - Fielded 900,000 middleware licenses
 - Fielded 2,000 Public Key Enabling Development kits
 - Trained 6,016 personnel to install readers & middleware, set up user certificates, and establish CAC logon procedures
 - Provided on site fielding and training to 103 separate locations
 - Answered 2,500 Help Desk calls
 - Conducted functional and operational testing of 12 separate card readers and 4 middleware products
 - Conducted multiple smart card, PKI, and biometrics pilots
- CAC/PKI Lessons Learned
 - CAC, like the PIV, is a personal identity card
 - PKI in this context, refers to cryptographic certificates
 - Information Technology and Personal Identity are different programs with different proponents
 - In DOD, personal identity, cryptographic certificates, and information technology are three different programs with different proponents
 - For Smart Card + PKI + Biometrics to work, one proponent needs to be in charge
- CAC Lessons - 2001
 - CAC not accepted as DoD ID Card (bars & borders)
 - Issuance Services were down 15% of the time
 - Issuance times too long
 - Users did not remember their PIN

- CAC Lessons - 2002
 - New smart card means new middleware
 - New smart card = new reader drivers
 - Installing readers and middleware was not a military priority
 - Most people forget to remove CAC from reader when they leave workspace
 - Users do not remember their PIN
 - Issuance times continued to be too long
 - Issuance infrastructure unreliable
- CAC Lessons - 2003
 - Post Issuance” support must be as close to the user as possible
 - Promised services never materialized
 - Issuance to remote and high volume users is a big problem
 - People forget to remove CAC from reader when they leave workspace
 - Users do not remember their PIN
 - Issuance times continue to be too long
 - Issuance infrastructure unreliable
- CAC Lessons - 2004
 - Promised PKI services never materialized
 - Issuance to remote and high volume users gets resolved
 - People forget to remove CAC from reader when they leave workspace
 - Users do not remember their PIN
 - Issuance times get shorter – hit 15 minute threshold
 - Issuance infrastructure becomes more reliable
- CAC Lessons - 2005
 - Promised PKI services start to materialize
 - People forget to remove CAC from reader when they leave workspace
 - Users do not remember their PIN
 - Issuance times good
 - Issuance infrastructure very reliable
 - Certificate Validation Services

K. Concluding remarks Mike Butler (IAB):

- Mike closed the meeting by offering thanks to all of the people that made the meeting a success:
 - Thanks to Greta Lehman of DoD for offering an entertaining, candid, and enlightening presentation.
 - Thanks to organizations, government, and industry for participating.
 - Thanks to the Smart Card Alliance for hosting our meeting
- Next session scheduled May 17th at the GPO Auditorium, which is near Union Station.
- A press wrap-up was held, and the meeting was adjourned at 12:10.